FORM PTO-1390 (REV 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: PA1317US

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): Unknown 09/554518

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US99/24157	October 14, 1999	October 14, 1998

TITLE OF INVENTION: System And Method of Authenticating A Key And Transmitting Secure Data

APPLICANT(S) FOR DO/EO/US: Lynn D. Spraggs

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C371(b) and PCT Articles 22 and 39(1).
4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [X] is not required, as the application was filed in the United States Receiving Ofice (RO/US).
6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [X] Amendments to the claims of the International Application under PCT Article 19(35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [X] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [X] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [ ] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:
    Verified Statement Claiming Small Entity Status;
    Petition to Make Special Because of Prospective Manufacture Under 37 C.F.R. 1.102; Statement In Support Of Petition To Make Special;
    Check to cover fee for Petition to Make Special ($130.00)

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
Unknown 09/554518	PCT/US99/24157	PA1317US

422 Rec'd PCT/PTO 11 MAY 2000

17. ☒ The following fees are submitted:	CALCULATIONS PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :	
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$970.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$840.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$690.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$670.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$96.00**	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 690.00
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	13 - 20 =	0	X $18.00	$ 0.00
Independent claims	3 - 3 =	0	X $78.00	$ 0.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $260.00	$ 0.00

TOTAL OF ABOVE CALCULATIONS =	$ 690.00
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also by filed (Note 37 CFR 1.9, 1.27, 1.28).	$ 345.00
SUBTOTAL =	$ 345.00
Processing fee of **$130.00** for furnishing the English translation later than ☐20 ☐30 months from the earliest claimed priority date (37 CFR 1.492(f)). +	$
TOTAL NATIONAL FEE =	$345.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$ 40.00
TOTAL FEES ENCLOSED =	$ 385.00
Amount to be refunded:	$
charged:	$

a. ☒ A check in the amount of $ 385.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pendin g status.

SEND ALL CORRESPONDENCE TO:

Aaron R. Wininger
Carr & Ferrell LLP
2225 East Bayshore Road Suite 200
Palo Alto, CA 94303

SIGNATURE:

Aaron R. Wininger
NAME

45,229
REGISTRATION NUMBER

Atty. Dkt.No. PA1317US

Applicant: Lynn Spraggs
PCT International Serial No.: PCT/US99/24157
PCT Filed: October 14, 1999
US Serial No. Unknown
For: System and Method of Authenticating a Key and Transmitting Secure Data

VERIFIED STATEMENT (DECLARATION) CLAIMING
SMALL ENTITY STATUS
(37 CFR 1.9 (f) and 1.27 (c)) - SMALL BUSINESS CONCERN

I hereby declare that I am:

[ ] the owner of the small business concern identified below:
[X] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN Ultra Information Systems LLC
ADDRESS OF CONCERN 1101 San Antonio Road, Suite 409
Mountain View, CA 94043

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.2, and reproduced in 37 CFR 1.9 (d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled "System and Method of Authenticating a Key and Transmitting Secure Data", by inventor Lynn Spraggs, as described in

[ ] the specification filed herewith.
[X] PCT application serial no. PCT/US99/24157, filed October 14, 1999.
[ ] patent no._____, issued _____.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e). *NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME _____

ADDRESS _____

[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28 (b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of the Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING ASHOK MATHUR

TITLE OF PERSON IF OTHER THAN OWNER Vice President & Co-Owner

ADDRESS OF PERSON SIGNING 1101 San Antonio Road, Suite 409
Mountain View, CA 94043

SIGNATURE _____ DATE 4/27/00

SYSTEM AND METHOD OF AUTHENTICATING A KEY AND TRANSMITTING SECURE DATA

BACKGROUND OF THE INVENTION

1. Field of the invention

The present invention relates generally to computer security and more specifically to allow the authentication of a key for the transmission of secure data between computers using the key.

2. Description of the Prior Art

In order to securely transfer data between computers on the Internet, various different types of encryption/decryption methods are used. One way of securely transferring data over the Internet includes the use of a public key/private key system.

A public key is provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures.

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority. The private key is given only to the

requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key counterpart by someone else who has the public key.

The private key is vital key to a user. If the private key is copied or stolen from the user, then secured data can be compromised as well as causing problems in properly authenticating the private key and the user using the private key.

Thus, it would be desirable to provide a system and method of authenticating a key so that the transmission of secure data using the key can be reliably originating from an authenticated key and/or an identifiable user.

SUMMARY OF THE INVENTION

A system and method is provided for authenticating a key of a user by decrypting an encrypted data file provided by the user with a password provided by the user into the authenticated key of the user. The encrypted data file can be stored on a RF smart card and can contain encrypted biometric data identifying the user, such as a fingerprint. An additional security measure can be used by taking a digitized biometric fingerprint scan of the user and probabilistically comparing the digitized fingerprint scan of the user with the authenticated key of the user. The user's key can then be used to securely encrypt and transmit data accordingly knowing that the key has been authenticated.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying illustrations. For simplicity and ease of understanding, common numbering of elements is employed where an element is the same in different illustrations.

FIG. 1 is a schematic diagram illustrating a user's key being authenticated prior to transmitting secure data over the Internet, in accordance with the present invention;

FIG. 2 is a block diagram of the client computer shown in FIG. 1, in accordance with the present invention;

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module located within the client computer of FIG. 2; and

FIG. 4 is a flowchart of a method illustrating the authentication of a key at a client computer, according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

Referring now to FIG. 1, a schematic diagram illustrates a web server 100 and a client computer 102 connected to the Internet 110. For security purposes, the client computer 102 has a RF reader (radio frequency reader) 104 for reading a RF smart card 106 having a user's private key. The private key on the RF smart card 106 can be very long (i.e. 1000 bytes) and could include any type of biometric data, such as a digitized fingerprint of the user. The private key could be very long and any data that is encrypted using this private key would be virtually impossible to decrypt by a hacker, since this private key can be much longer than a typical private key (64 bytes) used in a

private/public key system. The client 102 also has a fingerprint scanner 108 for helping to authenticate the private key of the user. Biometric readings employed by this invention are not limited to fingerprints. Other types of biometric readings can also be used, such as the reading from the eye and analysis of the face.

FIG. 2 is a block diagram of the client computer 102 shown in FIG. 1. Computer 102 includes a CPU 202, a RAM 204, a non-volatile memory 206, an input device 208, a display 210, an Internet interface 212 for providing access to the Internet, a RF reader interface 214, and a fingerprint scanner interface 216.

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the client computer 102 of FIG. 2. The non-volatile memory 206 includes an encrypt/decrypt engine 302 for encrypting and decrypting data.

The encrypt/decrypt engine 302 is programmed to encrypt and decrypt data using a password or a key. Excellent results can be obtained when using the blowfish algorithm for encryption and decryption. Other types of symmetric key encryption/decryption algorithms can also be employed within the encrypt/decrypt engine 302.

FIG. 4 is a flowchart of a method illustrating the authentication of a key at a client computer in accordance with the invention. The authentication process begins at step 400. The authentication process includes three security levels, however, not every level of

security is required to authenticate the key of the user. Depending on the type of application, only one or two of the security levels may be employed.

Security level I 402 begins at step 404 where the user scans his user's RF key card 106 with the RF reader 104. Security level II 406 then begins at step 408 where the user enters his password at the client computer 102. At step 410 the data scanned from the user's RF key card is decrypted with the encrypt/decrypt engine 302 using the user's password.

At step 414, security level III 412 begins and a digitized fingerprint scan is taken from the user. At step 416 the digitized fingerprint scan is compared with the data decrypted from the RF key card. At step 418 it is determined if there is a probabilistic match between the digitized fingerprint scan and the data decrypted from the RF key card. If it is determined that there is not a match, then at step 420 the authentication of the user's key fails and is rejected. If at step 418 it is determined that there is a match, then at step 422 the user's key is authenticated. The decrypted data from the RF key card can then be used as an authenticated encryption key for sending data to a server over and unsecure network, such as the Internet.

I Claim:

1. A system for authenticating a key of a user, comprising a decrypt engine for decrypting an encrypted data file provided by the user with a password provided by the user into the key of the user.

2. The system of claim 1, wherein the encrypted data file is stored on a RF smart card.

3. The system of claim 1, wherein the encrypted data file contains encrypted biometric data identifying the user.

4. The system of claim 3, wherein the biometric data includes a digitized fingerprint of the user.

5. The system of claim 3, further including a scanned biometric reading of the user, wherein the scanned biometric reading of the user is probabilistically compared with the key of the user in order to additionally authenticate the key of the user.

6. The system of claim 5, wherein the scanned biometric reading of the user is a fingerprint scan.

7. A method for providing an authenticated key of a user, comprising the steps of:

providing an encrypted data file;

providing a password; and

decrypting the encrypted data file using the password into an authenticated key of the user.

8. The method of claim 7, wherein the encrypted data file is stored an a RF smart card.

9. The method of claim 7, wherein the encrypted data file contains encrypted biometric data identifying the user.

10. The method of claim 9, wherein the biometric data includes a digitized fingerprint of the user.

11. The method of claim 9, further including the steps of:

scanning a biometric feature of the user; and

probabilistically comparing the scanned biometric feature of the user with the key of the user in order to additionally authenticate the key of the user prior to securely transmitting data using the key.

12. The method of claim 11, wherein the scanned biometric feature of the user is a fingerprint.

13. A computer-readable medium comprising program instructions for providing an authenticated key of a user, comprising the step of:

decrypting an encrypted data file provided by the user using a password provided by the user into an authenticated key of the user.

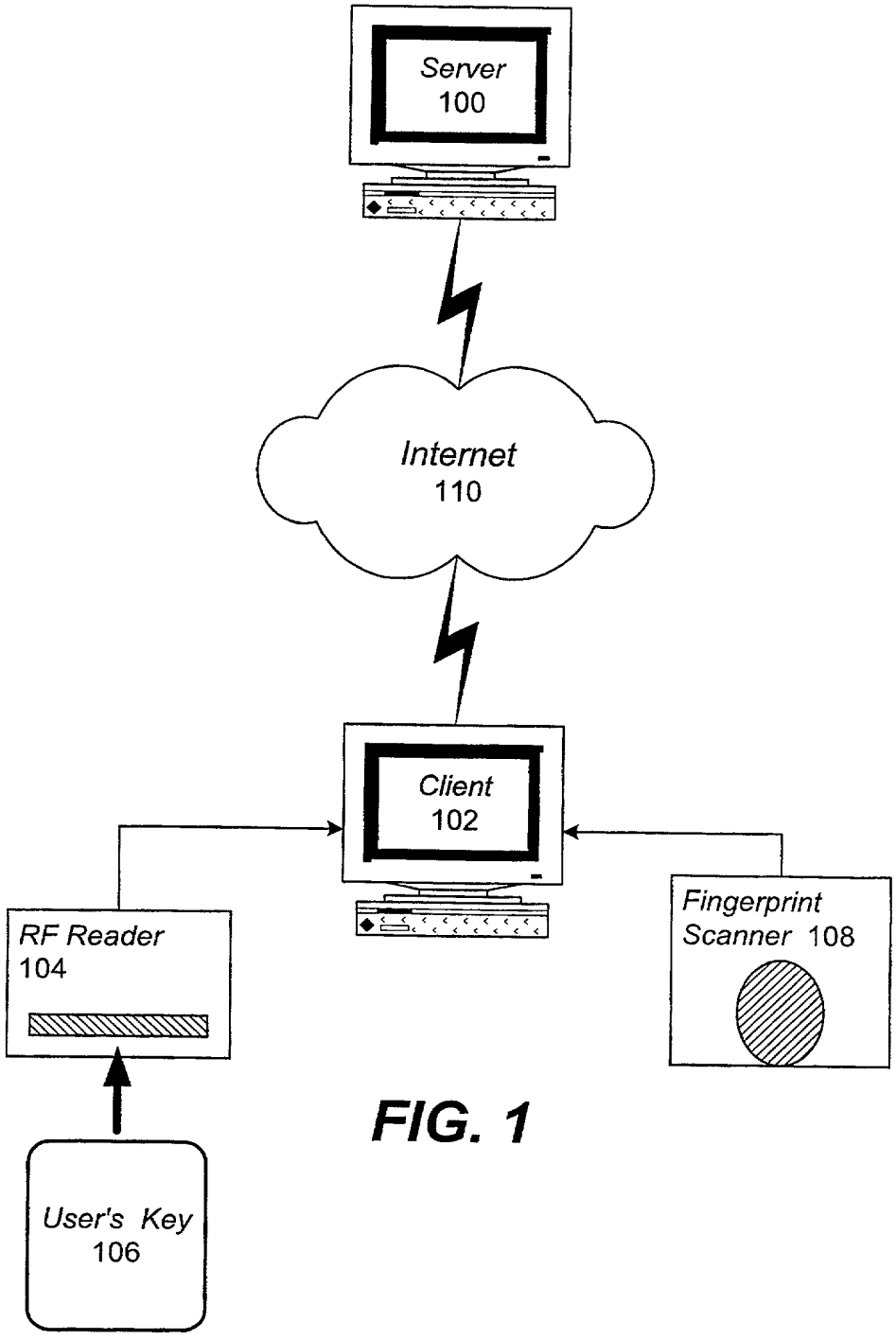
Server
100
Internet
110
Client
102
RF Reader
104
Fingerprint
Scanner 108
User's Key
106

FIG. 1

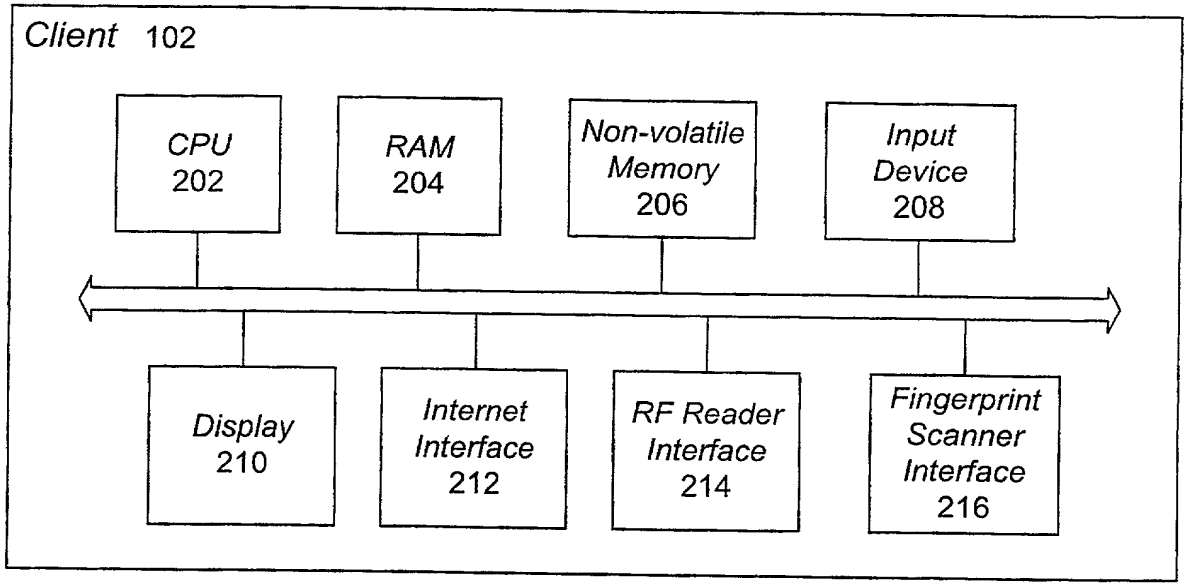
Client 102
CPU 202
RAM 204
Non-volatile Memory 206
Input Device 208
Display 210
Internet Interface 212
RF Reader Interface 214
Fingerprint Scanner Interface 216

FIG. 2

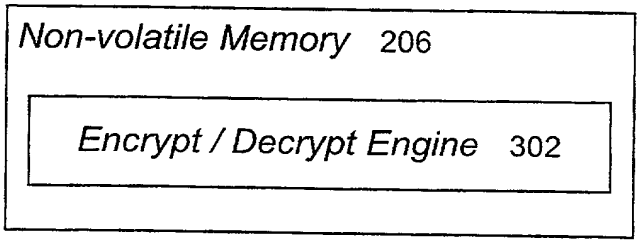
Non-volatile Memory 206
Encrypt / Decrypt Engine 302

FIG. 3

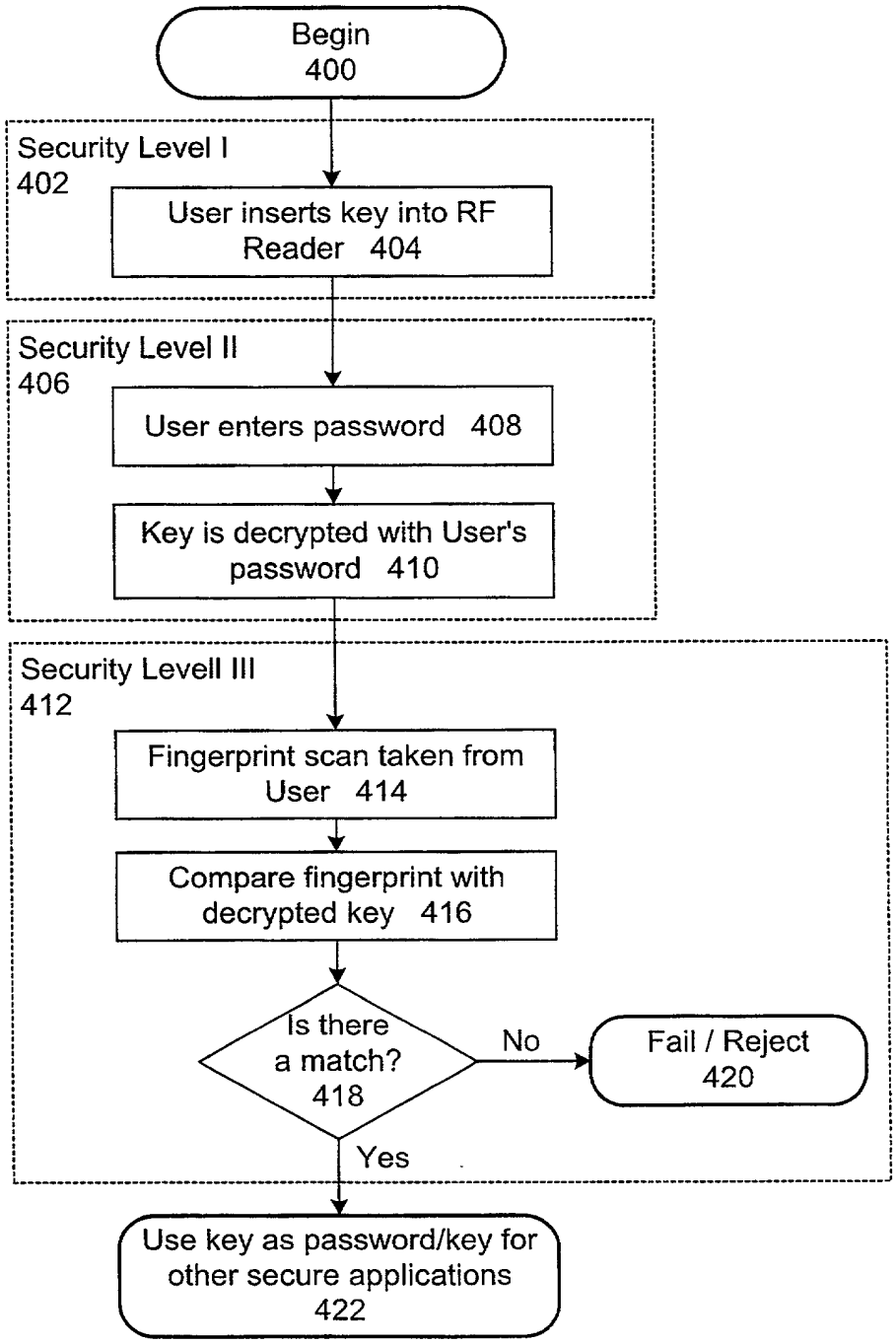
Begin
400
Security Level I
402
User inserts key into RF Reader 404
Security Level II
406
User enters password 408
Key is decrypted with User's password 410
Security Levell III
412
Fingerprint scan taken from User 414
Compare fingerprint with decrypted key 416
Is there a match?
418
No
Fail / Reject
420
Yes
Use key as password/key for other secure applications
422

FIG. 4

ATTORNEY'S DOCKET NO.: PA1317US

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **"System and Method of Authenticating a Key and Transmitting Secure Data,"** the specification of which (check one):

|__| is attached hereto.
|X| was filed on October 14, 1999
as U.S. Application No. _____
or PCT International Application No. PCT/US99/24157
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Claimed	
_____ (Number)	_____ (Country)	_____ (Day/Month/Year filed)	|__| Yes	|__| No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year filed)	|__| Yes	|__| No

I hereby claim the benefit under Title 35, United States Code §119(e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)
(Application Number)	(Filing Date)

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

PCT/US99/24157	October 14, 1999	Pending
(Application Number)	(Filing Date)	(Status -- patented, pending, abandoned)
(Application Number)	(Filing Date)	(Status -- patented, pending, abandoned)

POWER OF ATTORNEY: I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

John S. Ferrell, Reg. No. 34,593; J. Eppa Hite, Reg. No. 30,266; Gregory J. Koerner, Reg. No. 38,519; Charles B. Katz, Reg. No. 36,564; John D. Henkhaus, Reg. No. 42,656; Susan Yee, Reg. No. 41,388; Robert Toczycki, Reg. No. 38,341 and Aaron Wininger, Reg. No. 45,229.

SEND ALL CORRESPONDENCE TO:

Aaron Wininger
CARR & FERRELL *LLP*
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
TEL: (650) 812-3400
FAX: (650) 812-3444

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole inventor: LW Lynn Spraggs

Inventor's signature _____ Dated: 3/28/2000

Residence 8604 Kalavista Dr.

Post Office Address Vernon BC CAN Citizenship Canadian